# Navy
# Maritime
# Domain Awareness
# Concept

2007

# Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE **29 MAY 2007** | 2. REPORT TYPE | 3. DATES COVERED **00-00-2007 to 00-00-2007** |
|---|---|---|

| 4. TITLE AND SUBTITLE **Navy Maritime Domain Awareness Concept** | 5a. CONTRACT NUMBER |
|---|---|
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Navy,Chief of Naval Operations,Washington,DC** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **24** | |

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

IN REPLY REFER TO

MAY 2 9 2007

MEMORANDUM FOR DISTRIBUTION

Subj: MARITIME DOMAIN AWARENESS CONCEPT

Encl: (1) Navy Maritime Domain Awareness Concept (U)

1. The Navy Maritime Domain Awareness (MDA) Concept is approved for dissemination. It guides Navy efforts to improve MDA-related capabilities and develop related Fleet Concepts of Operations. This concept fully supports the National Security Presidential Directive for Maritime Security and the National Plan to Achieve MDA.

2. Enclosure (1) addresses applicability of MDA to the Navy warfighter at each level of command and presents a vision for the exchange and use of maritime information in support of maritime security and safety. We must integrate the goals in this document with the priorities of maritime stakeholders across interagency, commercial industry, and private enterprise.

3. The POC for the Navy MDA is CDR William Wimmer, N5MDA, at william.wimmer@navy.smil.mil or (703) 697-4081.

M. G. MULLEN
Admiral, U.S. Navy

Distribution:
CNO (N00,N09,N1,N2,N3/N5,N4,N6,N8)
CFFC (N00, N3/N5)
COMPACFLT (N00, N3/N5)
COMUSNAVEUR (N00, N3/N5)
COMUSNAVCENT (N011, N3/N5)
NAVY IPO (00/01/02/09)
ONR (00/ILO)
NETC (N00)
NWC (N00)
USNA (N00)
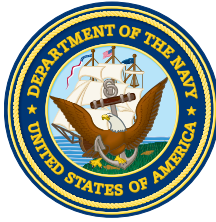
# Navy Maritime Domain Awareness Concept

## Purpose

This document provides overarching guidance for the development and application of Maritime Domain Awareness (MDA) across all levels of command for the United States Navy. It provides the conceptual framework to prioritize MDA efforts across Navy, ensure alignment with external MDA initiatives, and inform the Fleet MDA Concept of Operations (CONOPS). Classified elements to Navy's overall MDA Concept can be found in Appendix A, allowing widespread dissemination of the main document.

## Scope

The time horizon for fully implementing this concept is ten years. Efforts to improve MDA are ongoing. Initial progress may be slow, but will accelerate as barriers to broad-based information sharing are overcome. This concept does not encroach on roles and responsibilities of other agencies within the U.S. government. When working in the international arena, Navy will coordinate with appropriate U.S. government agencies and comply with applicable policy, standards and protocols. Particular attention will be given to close alignment with the Department of Defense (DoD) Chief Information Officer, the Departments of State, Homeland Security, Transportation and the Office of the Director of National Intelligence.

### Core Assumptions

- Acquiring and sharing maritime information with a broad array of partners reduces vulnerability to attack and improves cooperation toward maritime security and safety.

- U.S. agencies and international partners perceive positive return on investment and recognize benefits of cooperating to achieve common maritime security goals.

- Overcoming cultural and policy barriers to information sharing requires changes in business practices and information security procedures.

- Planned Maritime Headquarters with Maritime Operations Center (MHQw/MOC) process and communication improvements will enable key aspects of this concept.

- Costs to implement this concept will not be prohibitive.

# Background

Navy has recognized for some time that its operational focus was broadening from primarily blue water to include the littorals. Although regional conflict remains a prime concern, Navy is increasingly faced with non-traditional challenges such as disaster relief and irregular opponents who employ asymmetric methods and capabilities against U.S. interests. In under-governed areas of the global commons, such as the littorals of failed states, Navy confronts networked adversaries thriving in the "gray area" between criminal activity and armed conflict.



*Hundreds of oil tankers each year receive their payload from Iraq's Al Basrah Oil Terminal (ABOT). Navy photo by MC1 Richard J. Brunson*

Worldwide economic trends have accelerated the pace of maritime commerce and reinforced the need to keep the global maritime commons secure. The oceans are growing in importance as both arteries of the global economy and back alleys of the criminal underworld. The role of naval power in securing the maritime domain gains in prominence when viewed in context of economic growth promoting political stability. Commerce craves security. Improving maritime security and safety are cornerstones of the National Strategy for Maritime Security (NSMS) and hinge upon developing systems and processes that help the world community, the United States, and the U.S. Navy attain a keen understanding of maritime activity. Performing Maritime Change Detection, the identification of anomalies from established trends and patterns, will enable commanders to take appropriate action before security is compromised or crises erupt. This is a primary goal of MDA.

# Military Challenge

Navy missions encompass the full range of military operations (ROMO). These missions necessitate operations in both blue-water and the littorals, and present unique challenges to our naval forces. Navy's increased focus on the littorals precipitated an exponential increase in the volume of contacts and activity that must be understood.

Concurrently, the capability to process maritime information has not kept pace with the increased volume and the number of organic reconnaissance assets available to gather this information has declined. Figure 1 illustrates the trends.
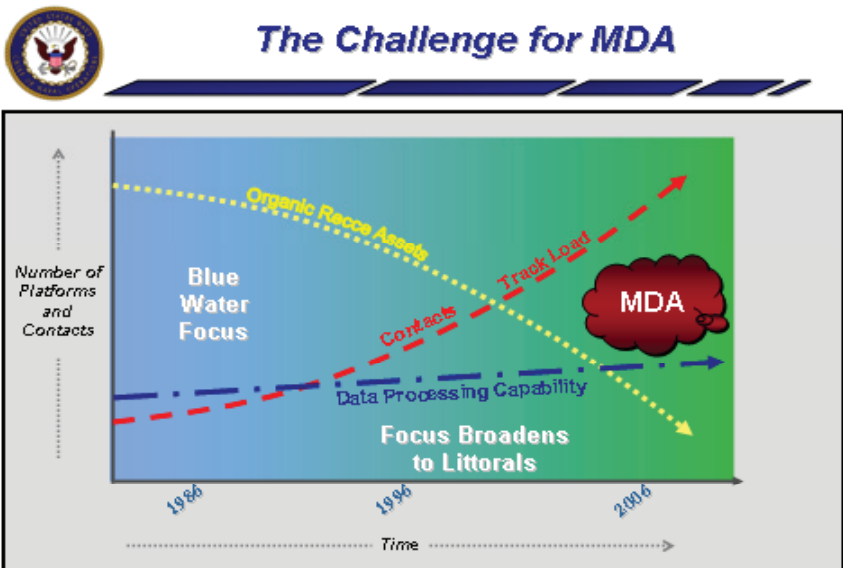


**Figure 1**

Transparency of activity in littoral regions and the global commons is requisite to understanding those environments and requires access to information historically unavailable to decision-makers at the operational and tactical levels of command. Information-sharing relationships with partner agencies and nations are vital to attaining the level of MDA that naval commanders require for effective decision-making at each level of command: Strategic, Operational and Tactical.

# MDA Defined

According to the National Plan to Achieve Maritime Domain Awareness: "Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States."

The National Plan also states the purpose of MDA: "to facilitate timely, accurate decision making that enables actions to neutralize threats to U.S. national security interests."

Effective understanding occurs when a decision-maker's comprehension of relevant information allows him to take appropriate action. From a U.S. Navy perspective, MDA consists of what is observable and known (Situational Awareness), as well as what is anticipated or suspected (Threat Awareness). It occurs when these two components are brought together to provide a decision-maker with an amalgamation of operational, intelligence and environmental information. Viewed in light of Navy's worldwide presence, MDA translates to: Global Maritime Situational Awareness (GMSA) plus Maritime Threat Awareness.

The term "effective understanding" acknowledges that information requirements vary depending upon the mission or task at hand. Therefore, MDA equates to understanding of the content, activity patterns, changes, and potential threats in the maritime environment that a commander (decision-maker) needs to perform the broad array of Navy missions.

The following attributes provide a practical understanding of Navy's perspective toward MDA:

| What it is: | What it isn't: |
|---|---|
| - Global | - Just homeland |
| - Coalition/International | - U.S. Only |
| - Joint & Interagency | - Just Defense |
| - Security Partnerships | - Just vessel tracking |
| - Information Sharing | - Just intelligence |
| - All threats | - Just terrorism |
| - Origin to delivery | - Just more sensors |
| - A continual process | - An end state |

# Navy Contribution to National MDA

The NSMS and its eight supporting plans, approved by the President in 2005, direct all U.S. government departments and agencies with a stake in the maritime domain to improve their organic processes and capabilities, and eliminate barriers to information-sharing in order to more fully safeguard vital U.S. national security interests in the maritime domain. The National Plan to Achieve MDA formally established a National MDA



*An Aviation Warfare Systems Operator takes a photograph of an unidentified oil tanker.*

Implementation Team (MDA-IT) to develop a National MDA CONOPS and an interagency MDA Investment Strategy. Navy, as a member of the National MDA-IT, is integrally involved in the ongoing development of the National MDA CONOPS and Investment Strategy.

Navy makes a very substantial and multi-faceted contribution to the U.S. Maritime Domain Awareness initiative in the form of:

- information and intelligence gathered by forward-deployed naval forces;
- analytic capability provided by the Office of Naval Intelligence (ONI) as the principal resident within the National Maritime Intelligence Center (NMIC) at Suitland, Maryland;

- a global command, control and communication network that links our tactical units and operational headquarters with U.S. strategic and interagency maritime stakeholders;
- invaluable information-sharing relationships with many international and commercial maritime partners;
- persistent Naval Criminal Investigative Service (NCIS) presence in many overseas ports;
- robust Theater Security Cooperation (TSC) initiatives including military personnel exchange and training programs;
- extensive combined exercise programs focused on maritime security.



*Members of the Visit, Board, Search and Seizure (VBSS) Team assigned to guided missile cruiser USS Monterey (CG 61) conduct a boarding of a merchant ship.*

Navy remains committed to U.S. maritime security through exploration of new and innovative technologies, removal of policy impediments, and leadership to promote a culture of information sharing. Navy will continue to work with the U.S. Coast Guard, inter-agency, and international partners to improve the security of the global maritime commons. Navy will support U.S. government efforts to establish a national maritime common operational picture (NMCOP), envisioned in the National Plan to Achieve MDA as the primary method for sharing maritime information across the government. Administration of the NMCOP and determination of access restrictions will occur outside of the Department of Defense. Instrumental to both national and regional maritime information networks, Navy will:

- ensure that NMCOP development is compatible with the burgeoning global framework of regional maritime situational awareness (RMSA) networks;
- leverage its unique position to foster growth, harmonize function, and draw on the content of each to deliver robust situational awareness (SA) to naval commanders;
- recommend amendment, as necessary, to national policy regarding MDA, compatibility with the NMCOP and contributions to international maritime networks.

# Navy Vision for Global MDA

No nation, let alone a single agency, has the capability or capacity to achieve MDA unilaterally. MDA requires broad collaboration among many partners, each with a potentially vital contribution to effective understanding of the maritime domain. Navy's vision for global MDA contains these primary elements:



Global network of regionally based maritime information exchange partnerships.

A baseline situational awareness of the maritime domain, essential to fostering cooperation and collaboration among maritime security providers, will emerge when participating nations, and other actors, voluntarily contribute to unclassified RMSA networks. Linking RMSA networks creates a global

MDA framework that facilitates global maritime security cooperation. Globally networked MHQ w/MOCs will effectively link RMSA pictures and improve the unity of operations and intelligence efforts across the full-spectrum of maritime missions from tactical to strategic.

For RMSA networks to fulfill their role as building blocks for GMSA, they must possess low barriers to entry, a stable technology base, and protocols to exchange unclassified information (such as Automatic Identification System (AIS) positions, crew lists and cargo manifests). Incentivizing others to contribute data relevant to Navy missions requires that we make available information relevant to partner concerns.

<u>Institution of worldwide standards for broadcast of vessel position and identification.</u>

The force structure needed to surveil U.S. maritime approaches actively, let alone the global commons, is unaffordable. The alternative is to establish standards for universal broadcast of identification and position information. Domestic and international regulatory changes will be necessary to maximize vessel compliance and ensure accuracy of vessel identity information. Acquiring GMSA will be greatly facilitated by the emergence of an international construct that can set standards for broadcast and sharing of information related to maritime safety and security, analogous to what the International Civil Aviation Organization (ICAO) does for international aviation. Vessel compliance relies on appropriate commercial incentives and availability of inexpensive position and identification broadcast equipment. Navy supports U.S. Coast Guard efforts for legislation that mandates use of these systems in U.S. waters.

<u>Automated tools that discern patterns, changes, and potential threats.</u>

MDA requires capabilities and processes to discover potential maritime threats as they materialize. The tremendous amount of maritime information and dedicated intelligence capability available within U.S. government and RMSA networks will provide naval commanders a solid grasp of the regional and cultural norms within their operating areas, and enable them to discriminate anomalous or suspicious behavior. Discerning potential maritime threats through this type of analysis, known as Maritime Change Detection, requires significant upgrades in automated data management technology.

<u>Alerting maritime partners of suspicious behavior and potential threats.</u>

Afloat commanders, host nations, and commercial carriers must be quickly alerted to suspicious activity or potential threats. As RMSA networks mature, they may become the mechanism that brings together situational awareness and threat awareness for participants. Partners that become aware of suspicious behavior or potential threats can alert others in the network by "spotlighting" suspect vessels in the system. This capability will entice others to join the RMSA network and enhance overall maritime security efforts.

# Global Maritime Situational Awareness

A precondition to true MDA, and to successful execution of many of Navy's worldwide mission sets, is establishment of robust GMSA: a multi-layered, multi-domain picture that links the identity, location, known patterns and present activity of ships, cargo, people, and hazards within and adjacent to the maritime domain. This picture derives from the pooling of a comprehensive set of mostly unclassified data contributed by the many agencies and nations with knowledge of the maritime domain. It is a compilation of information, regardless of classification, ranging from environmental data (oceanographic, meteorological, etc.) to vessel positions and characteristics, to cargo manifests and supply-chain information, to biometric identification data, to regional activity patterns (fishing areas, commercial routes, seasonal variations, etc.). While not all-inclusive, this list illustrates the depth and complexity of maritime information contributing to GMSA and that it far exceeds what can be gathered by Navy organic sensors alone.

# Maritime Threat Awareness

Anticipating the actions of others in the maritime domain, whether malevolent or benign, is fundamental to the MDA a naval commander needs to make appropriate and timely decisions. Often, Navy commanders must discern maritime threats in their operating area based solely on information at hand, without the benefit of unambiguous intelligence. This requires continuous assessment of the operating area, in context of the anticipated threat environment, to detect anomalous or suspicious behavior that may correlate to potential threats. Accurate assessment of trends and anomalies requires deep knowledge of the anticipated threat. SA alone does not

provide effective understanding of the maritime domain, nor does it enable a commander to position his forces optimally to respond to potential or emergent threats. Knowledge of the maritime threat is derived fusion of all-source information and intelligence against a backdrop of expertise on regional and cultural norms.



*USS Winston S. Churchill (DDG 81) follows a suspected pirate vessel in the Indian Ocean.*

Forensic analysis has discovered that most terrorist activity is preceded by criminal events or aberrant behavior. Correlating seemingly unrelated criminal activity with anomalous maritime behavior requires continuous assessment of the maritime domain and automated tools that alert commanders when suspicious items are uncovered.

## Enabling Navy Operations

As the world's premier maritime force, Navy's capabilities, systems and capacity are favorable for forecasted force-on-force requirements. Navy ability to locate, track, and anticipate the actions of a military adversary has been honed over decades and is unsurpassed. Yet, for the foreseeable future, Navy will face threats that arise not only from a military competitor, but from irregular, non-traditional opponents. Attempting to secure the global commons is futile if we cannot see the threat, whether in support of the War on Terror or as part of Major Combat Operations. Effective inte-

gration of capabilities supporting information and intelligence collection, operations, and communications is crucial to obtaining decision superiority and achieving a comprehensive understanding of threats in the maritime domain.



*A Visit, Board, Search and Seizure (VBSS) team departs the Panamanian-flagged Motor Vessel Hayder after conducting a security sweep of the ship. Hayder contacted the guided missile cruiser USS Cape St. George (CG 71) via bridge-to-bridge radio reporting it had been fired upon and illegally boarded in the Northern Persian Gulf.*

As an instrument of national power, Navy is increasingly called upon to perform maritime security operations while deterring regional aggression and denying the use of the maritime domain to international terrorist organizations. Maritime Domain Awareness is a critical enabler for the full range of naval missions and maritime security responsibilities.

The Naval Operating Concept presents a vision for current and emerging Navy missions in support of U.S. strategic maritime objectives. Complementing and resulting from forward naval presence, MDA contributes directly to achieving each of the following strategic objectives:

### *Secure the United States from direct attack by confronting early and at safe distances, those who would threaten us.*

Critical to an effective defense-in-depth posture is the ability to interdict

threats to U.S. interests abroad.  Inherent to MDA is the detection of changes in maritime trends that indicate emergence of potential threats to global interests overseas, the maritime transportation system and freedom of navigation.  Early threat detection and interdiction adds time and space to potential response options, affording defense-in-depth and optimizing the advantages of naval forces.

***Secure strategic access and retain global freedom of action by ensuring that key regions, lines of communication and the global commons remain accessible to all.***

Requisite to a focused, effective response to any perceived maritime threat is transparency of activity in the maritime domain.  MDA pursues transparency of maritime activity on a global scale to support the free flow of commerce.

***Strengthen existing and emerging alliances and partnerships to address common challenges.***

Security for maritime commerce, and the transportation system upon which it relies, is a common goal for all participants in the global economy.  Maritime security is threatened by transnational threats such as drug trafficking, illegal arms trade, poaching, unlawful immigration, piracy, environmental sabotage and terrorism.  As with maritime security itself, MDA on a global scale is beyond the capacity of any single nation.  Collaboration to attain MDA and maritime security provides a framework for cooperation that is applicable to a host of other common challenges.

***Establish favorable security conditions by countering aggression or coercion targeted at our partners, interests, and operating forces – including coalition.***

MDA enables leaders at all levels of command to make effective decisions regarding force disposition to deter or counter aggression or coercion by our adversaries.  Applicable to strategic influencing, operational maneuver, or tactical employment, MDA contributes directly to maritime dominance by facilitating decision-making superiority and by enabling the selection and execution of the most appropriate response to any emerging threat.

*An Unmanned Aerial Vehicle (UAV) Scan Eagle launches from the flight deck aboard the amphibious assault ship USS Saipan (LHA 2).*

# MDA at the Strategic Level

At the strategic level, MDA contributes to U.S. efforts to shape and influence the global security environment. This will occur through invigoration of RMSA networks that can be seamlessly linked to support the common challenge of maritime security. Through meaningful participation in maritime security cooperation efforts such as MDA, Navy fosters trust and confidence in other TSC initiatives.

Facilitating regional partnerships that contribute to global maritime security and safety must occur with full recognition and acceptance of the fact that our allies and partner nations may not share all goals, but will normally find common ground in the area of countering transnational threats. Understanding and incorporating the goals of potential partners into our MDA and maritime security efforts is imperative to obtaining their cooperation. Maritime Security Cooperation is an organizing principle that supports legal activities (freedom of navigation, environmental and natural resource protection, energy security) while preventing the illegal exploitation or illicit use of the maritime domain.

Central to Navy's TSC effort is building partner nation capacity and

capability regarding maritime security and safety. While this may include providing partners with technical advice, and in some cases equipment and training, regarding participation in RMSA networks, Navy's principal contribution to these networks will be in the form of useful and timely maritime information. Foreign Area Officers (FAOs) can help determine the best incentives to gain regional partner contributions to RMSA networks that are relevant to Navy missions.

A core tenet of this concept is that Navy will share information and intelligence at all classification levels with appropriate partners. Overcoming barriers that inhibit Navy networks and command and control (C2) systems from sharing data with interagency, international, and commercial entities requires:

- reevaluation of policy regarding assignment of security classification and access restrictions to maritime information;
- a culture of information-sharing fostered by adoption of a "write to release" work premise that maximizes the amount of data available for broad distribution;
- championing efforts to push maritime information to the lowest possible classification level, while protecting its source;
- development of automated multi-level security access devices and protocols;

These steps will maximize the amount of maritime information our Navy can freely contribute, and directly incentivize participation in RMSA network partnerships.

Building and nurturing partnerships is also vital to improving our intelligence collection capabilities. Bilateral and multilateral intelligence partnerships are often based on broader relationships forged at the national level, or result from other data-sharing agreements as trust builds over time. These intelligence relationships are fundamental to Navy's ability to gather data - both classified and unclassified - that might otherwise be unavailable. In pursuit of new sources of maritime information, Naval Intelligence will assist the Office of the Director of National Intelligence (ODNI) to:

- eliminate barriers to sharing of information and intelligence;
- adjust regulations that prevent merging "law enforcement sensitive" with other data;
- integrate private-sector and international partner data;
- declassify data whose intelligence source or method can be safely masked;
- leverage the capabilities of counterpart agencies and international partners to provide maximum flexibility to Navy operational users and decision-makers.

Automating access to maritime information dispersed throughout the U.S. government will require adoption of shared metadata standards that translate legacy maritime data sources into a common information pool. This information-sharing environment will make here-to-fore-inaccessible data available to operators and analysts at each level of command, and give them the ability to create a user-defined picture. Applying this model to both unclassified and secure networks means that, initially, two user-defined pictures will exist side-by-side in many operational and analysis centers. Eventually, multi-level security access will allow an individual to customize a single, fused "picture" of relevant maritime information and intelligence pulled from across the government. Information within RMSA networks will also be accessible. Implementing this model requires identification of an "information steward" to:

- interact with interagency and international counterparts to formulate metadata standards;
- provide technical expertise in retrofitting data holdings to adopted standards;
- ensure compliance Navy-wide;
- revisit data standards and architecture periodically to adapt to new requirements.

# MDA at the Operational Level

Navy focal points for MDA at the operational level of command will be Navy Component Commander, Numbered Fleet Commander and other designated Navy Headquarters, which are evolving to become MHQ w/ MOCs. Information requirements at this level vary because what is needed

during a regional conflict is dramatically different than for disaster relief or humanitarian assistance. This also holds true for required intelligence support.

Creating synergy between operations, intelligence, and information warfare functions, MHQ/MOCs will enable rapid decision-making in response to emerging threats. The following attributes make MHQ/MOCs ideally suited to become regional, operational-level MDA nodes:

- seamlessly networked with their counterparts in other theaters and regions, they will share relevant information and be mutually supportive;
- structured to gather, archive, and disseminate regional-specific maritime information;
- positioned to manage tactical unit access to the NMCOP or partner networks;
- possess up-echelon and regional connections that can enrich Navy's C2 system with maritime information useful to mission execution at the tactical level;
- established relationships with regional partners that provide an avenue to ensure Navy contribution to RMSA networks meets participant needs.

Leveraging Fleet Information Operations Centers, various theater and national collection capabilities, and other resources, intelligence professionals at MHQs will work with their operational counterparts to penetrate and pressurize clandestine networks and hard targets. Developing deep regional subject matter expertise to provide operational commanders with knowledge of adversary norms, patterns, and tactics will require significant upgrades to our signals exploitation capabilities, to include specialized training and the automated fusion and correlation of maritime data.

The centerpiece for MDA at the operational level is a C2 system capable of sharing maritime information among participants, integrating unclassified and classified data, and displaying it in a manner defined by the particular user. Fully capitalizing on regional and interagency information-sharing partnerships requires that this C2 network do the following:

- protect information from unauthorized access;

- permit free exchange of non-classified data and select restricted or classified information with regional partners and RMSA networks;
- correlate and fuse relevant maritime information;
- archive maritime information to enable Maritime Change Detection and  maintain a continuous level of SA as participants in the system change;
- provide an effective collaborative environment for Navy and other maritime partners.

Information in Navy's C2 system must be current, accurate, and tailor-able to the needs of the user.  Automated data fusion and correlation is essential to focus time and effort on understanding the information, rather than its management.  Embedded suspicion algorithms, continuously scanning current and archived maritime information, will enable Navy Component Commanders to alert assigned units, commercial entities, or host nations of potential threats.

# MDA at the Tactical Level

Growing emphasis on security in the global maritime commons means that Navy ships will continue to operate extensively in littoral regions and will increasingly need to coordinate their efforts with less capable partners. Combining acute SA with accurate intelligence allows Strike Group and unit commanders to assess activity accurately in congested environments, dominate tactical situations rather than merely responding to events after the fact, and possess a decided advantage over adversaries relying on stealth and surprise.

Strike Groups, ships and aircraft, and shore facilities constantly gather data regarding their operating environment.  Optimizing collection of information that leads to identification of suspicious maritime behavior requires thorough integration of intelligence with operational forces at the tactical level.  For example, maritime security-related data collection is enhanced by embedding intelligence personnel with Navy Special and Expeditionary Warfare Teams and incorporating specialized Intelligence Exploitation Teams into Maritime Interception Operations.

The inability to exchange SA information efficiently and effectively at the

*A member of Visit, Board, Search and Seizure (VBSS) team, assigned to the dock landing ship USS Carter Hall, climbs down to a Rigid Hull Inflatable Boat (RHIB).*



*MIO Operations in the Arabian Gulf*

tactical level is a major impediment to MDA. Afloat units must be able to augment their organic sensors with maritime information from resources at the operational and strategic levels. Equally important, they must be able to

rapidly transfer SA information up-echelon and to each other, as necessary. Improving MDA at the tactical level requires:

- more efficient collection and processing of maritime information at the unit level;
- near-real-time access for afloat units to collection, planning, and subject matter expertise at the MHQ w/MOC, Joint Intelligence Operations Center (JIOC) and NMIC;
- efficient transfer of SA information collected afloat, such as Maritime Interdiction-related data, up-echelon to the MHQ w MOC, the Office of Naval Intelligence (ONI), and other agencies where it can be analyzed, catalogued and archived;
- near-real-time exchange of select SA information to RMSA networks;
- real-time exchange of current and accumulated SA information to other tactical users, including less-capable partners.

While integration of information into Navy's C2 system from RMSA networks and up-echelon sources will occur at the MHQ, full tactical exploitation of this developing capability requires that unit-level applications be optimized for the bandwidth constraints characteristic of the maritime domain. As Navy networks migrate toward a service-oriented architecture, afloat use of internet-based tools and services will require reevaluation of existing security policy.

Proliferation of unclassified RMSA networks and development of the U.S. interagency maritime information-sharing environment will make available tremendous amounts of data. Fusion of organic sensor data with imported maritime information is necessary to provide tactical-level decision-makers with effective understanding of their operating environment. Presently, ships manage multiple maritime displays: an organic sensor display, a tactical picture (Link 11 or Link 16), a regional non-real-time COP (GCCS-M), and many are receiving stand-alone AIS input. Integrating these data and information streams is a labor-intensive process that yields inconsistent reporting of contact information, significant time latency, and incomplete SA available to tactical and operational commanders. Improving the ability of tactical units to create and use SA involves automating, as much as possible, the process of integrating these multiple perspectives.

The goal for MDA at the tactical level is to permit operators access to

information, regardless of source, associated with each contact in an integrated display.

# **Organizing for Success**

This concept makes clear that MDA contributes to a broad array of Navy missions and appeals to wide variety of stakeholders, inside and external to Navy. Successful implementation of this concept requires marshalling a complex set of activities, processes, systems and agencies to deliver effective MDA to Navy decision-makers. The magnitude of this effort exceeds the capacity or expertise of any single Navy directorate. Employing MDA to accelerate Navy's decision-making processes involves dedicated efforts to:

1.  Determine Navy requirements for MDA;
2.  Establish relationships requisite to accessing and sharing information;
3.  Identify and obtain relief from policies that hinder information access;
4.  Break down cultural barriers to sharing information;
5.  Solve technical challenges associated with information-sharing;
6.  Automate systems and processes to collect, manage, disseminate and display information;
7.  Modify training, planning and operational decision-making processes to capitalize on greater access to information

Managing development of MDA for Navy and influencing the direction of external MDA initiatives demand the creation of a cross-functional team (CFT) capable of capturing Navy strategic and policy perspectives, fleet operational requirements, and acquisition expertise from across the service.
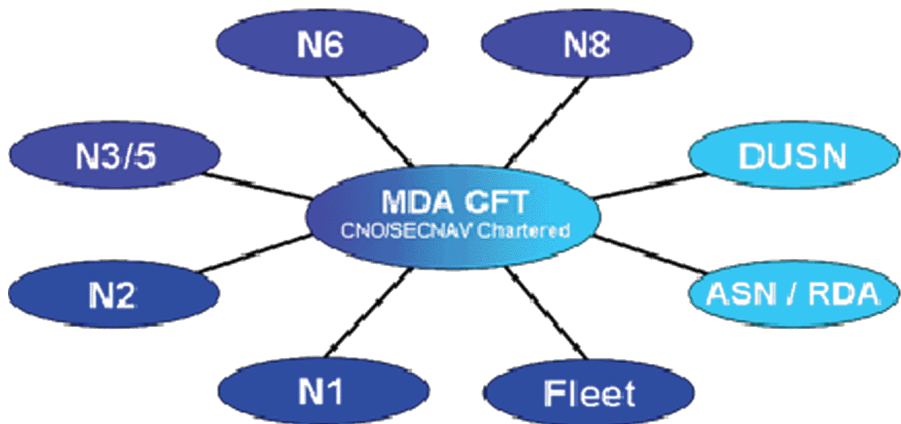
**Figure 2**

*Figure 2 illustrates a Navy MDA CFT that captures appropriate representation from the Fleet, Chief of Naval Operations (CNO) directorates, and the Secretary of the Navy (SN) staff. This organization will assess and rationalize Navy MDA efforts and set priorities regarding policy, procedures and procurement. By forging Navy-wide consensus the CFT can ensure that Navy MDA efforts remain congruent with interagency and international MDA initiatives. For success, the CFT requires authority drawn from SN and CNO.*

# Implications

This concept presents challenges for the next generation of C2 networks. Accelerating decision-making at each level of command requires these networks to access, filter, and deliver enormous amounts of maritime information in a useful and executable manner.

This concept envisions technological advances to automate critical information management processes. Until this occurs, some elements in this concept must be performed manually – impacting manning requirements at all levels of command, and potentially increasing costs of implementation. To keep costs manageable, phased implementation of this concept may be necessary. Implications for the operations, allocation and overall structure of naval forces are, as-yet, unforeseen, but may be derived from subsequent Fleet MDA CONOPS development.

This concept implies a broader acceptance of the comparative advantages offered by maritime partners. Substantial reliance on partner capabilities in lieu of developing them organically has implications that reverberate throughout Navy Strategy, and potentially U.S. National Defense Strategy.